

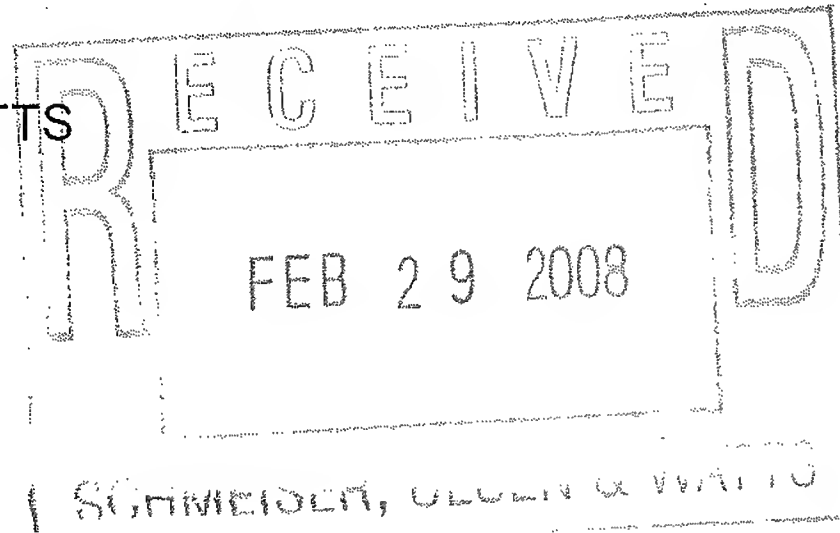
# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
10/539,648	12/17/2007	2131	1500	GB920020055US1	27	4

CONFIRMATION NO. 6660

30449  
SCHMEISER, OLSEN & WATTS  
22 CENTURY HILL DRIVE  
SUITE 302  
LATHAM, NY 12110



## FILING RECEIPT



Date Mailed: 02/27/2008

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Filing Receipt Corrections. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

### Applicant(s)

John Owlett, Hampshire, UNITED KINGDOM;  
George M. Thompson, Hampshire, UNITED KINGDOM;  
Keith A. Walton, London, UNITED KINGDOM;

### Assignment For Published Patent Application

INTERNATIONAL BUSINESS MACHINES CORPORATION, ARMONK, NEW YORK,

**Power of Attorney:** The patent practitioners associated with Customer Number 30449

### Domestic Priority data as claimed by applicant

This application is a 371 of PCT/GB03/05107 11/24/2003

### Foreign Applications

UNITED KINGDOM 0229894.1 12/21/2002

**If Required, Foreign Filing License Granted:** 08/28/2006

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 10/539,648**

**Projected Publication Date:** 05/29/2008

**Non-Publication Request:** No

**Early Publication Request:** No

**Title**

Methods, Apparatus And Computer Programs For Generating And/Or Using Conditional Electronic Signatures For Reporting Status Changes

**Preliminary Class**

380

**PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

**LICENSE FOR FOREIGN FILING UNDER****Title 35, United States Code, Section 184****Title 37, Code of Federal Regulations, 5.11 & 5.15****GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

#### **NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of: Owlett et al.

Serial No.: 10/539,648

Filing Date: 12/17/2007

Art Unit: 2131

Dkt. No.: GB920020055US1

Title: METHODS, APPARATUS AND COMPUTER PROGRAMS FOR GENERATING  
AND/OR USING CONDITIONAL ELECTRONIC SIGNATURE FOR REPORTING STATUS  
CHANGES

Confirmation No.: 6660

Commissioner for Patents

Office of Initial Patent Examination

Filing Receipt Corrections

P.O. Box 1450

Alexandria, VA 22313-1450

**CORRECTION OF FILING RECEIPT**

Sir:

Applicants respectfully request correction of the filing receipt for this case as indicated on the attached copy of the filing receipt. Please correct the total number of claims to read –26 –.

Consideration of the foregoing in relation to this patent application is respectfully requested.

Respectfully submitted,

Date: March 14, 2008

/Jack P. Friedman/

Jack P. Friedman

Reg. No.: 44,688

Customer No.: 30449

SCHMEISER, OLSEN & WATTS

22 Century Hill Drive, Suite 302

Latham, NY 12110

Phone: (518)220-1850

Fax: (518)220-1857

**In the Claims:**

Please amend claims 3, 5, 7-10, 12-15, 20, and 22-23. The claims are as follows.

1. (Original) A method for generating a conditional electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item, the method comprising the steps of:

encrypting the data item,

encrypting the one or more conditions separately from the data item, combining the encrypted data item and the encrypted one or more conditions, and

encrypting the combination to generate a digital signature block that inherently represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions.

2. (Original) A method according to claim 1, wherein each of a plurality of specified conditions is separately encrypted and combined with the encrypted data item, and wherein the combination is then further encrypted.

3. (Currently Amended) A method according to claim 1 ~~or claim 2~~, wherein the encryption of the data item and separate encryption of the conditions are each one-way hashing steps to generate verifiable representations of the data item and conditions.

4. (Original) A method according to claim 3, wherein the step of combining the hashed data item and conditions comprises concatenating the hashed data item and hashed conditions, hashing the product of the concatenation to produce a final digest, and further encrypting the final digest to generate a digital signature block.

5. (Currently Amended) A method according to claim 1 ~~or claim 2~~, wherein the step of encrypting the combination uses an encryption method for which the result of (a) combining the encrypted data item and the encrypted one or more conditions and then encrypting the combination differs from a result of (b) encrypting both the encrypted data item and the encrypted one or more conditions and then combining the doubly encrypted data item and conditions.

6. (Original) A method according to claim 5, wherein the encryption method implements Cipher Block Chaining encryption.

7. (Currently Amended) A method according to claim 1 ~~or claim 2~~, wherein the encryption of the data item and separate encryption of the conditions each use Cipher Block Chaining encryption methods.

8. (Currently Amended) A method according to ~~any one of the preceding claim~~ claim 1, wherein the step of encrypting the combination to generate a digital signature block uses a private key of a public/private key cryptographic solution to produce a conditional signature.



9. (Currently Amended) A method according to ~~any one of claim[[s]] 1 to 7~~, wherein the step of encrypting the combination to generate a digital signature block uses a symmetric key of a symmetric-key cryptographic solution to produce a conditional signature.

10. (Currently Amended) A method according to ~~any one of the preceding claim[[s]] 1~~, including the step of transmitting to a recipient the data item, the one or more conditions and the digital signature block, such that a recipient, who has access to the cryptographic processes used for performing the encrypting steps and has access to a corresponding decryption key, is enabled to:

decrypt the digital signature block to produce a first result;

encrypt the data item, encrypt the one or more conditions separately from the data item, and combine the encrypted data item and encrypted one or more conditions to produce a second result; and

compare the first and second results to determine whether they match.

11. (Original) A method according to claim 10, including transmitting the encryption algorithms to the recipient.

12. (Currently Amended) A method according to claim 10 ~~or claim 11~~, including transmitting to the recipient the interim results of each encryption step, comprising:

the encrypted data item; and

the encrypted one or more conditions.

13. (Currently Amended) A method according to ~~any one of claim[[s]] 10 to 12~~, wherein the step of encrypting the combination to produce a digitally signed data block uses a private key of a public/private key cryptographic solution, and wherein the method includes transmitting to the recipient the public key of the cryptographic solution.

14. (Currently Amended) A method according to ~~any one of claim[[s]] 10 to 12~~, wherein the step of encrypting the combination to produce a digitally signed data block uses a private key of a public/private key cryptographic solution, and wherein the method includes transmitting to the recipient information for obtaining the public key of the cryptographic solution.

15. (Currently Amended) A method according to ~~any one of claim[[s]] 10 to 14~~, including compiling a set of encryption results which set includes the results of each step of encrypting, and wherein the step of transmitting includes the step of transmitting the set of encryption results to the recipient.

16. (Original) A method according to claim 3, including the step of transmitting to a recipient the hashed representations of the data item and conditions and the digital signature block such that a recipient, who has access to the cryptographic process used to perform the step of encrypting the combination and has access to a corresponding decryption key, is enabled to:

decrypt the digital signature block;

combine the hashed representations of the data item and conditions to generate a combined digest; and



compare the decrypted signature block with the combined digest to determine whether they match.

17. (Original) A method according to claim 16, wherein the step of combining the hashed representations to generate a combined digest comprises the steps of:

concatenating the hashed representations to generate a double digest; and  
hashing the double digest to generate a final combined digest.

18. (Original) A method according to claim 1, wherein each of a plurality of data items is separately encrypted and combined, and the combination is then further encrypted.

19. (Original) A method for verifying a conditional electronic signature, generated by a method according to claim 10, comprising the following steps performed in response to receipt by the recipient of the transmitted data item, one or more conditions and the digital signature block:

decrypting the digital signature block to produce a first result;  
encrypting the data item, encrypting the one or more conditions separately from the data item, and combining the encrypted data item and encrypted one or more conditions to produce a second result; and  
comparing the first and second results to determine whether they match.

20. (Currently Amended) A computer program product loadable into the internal memory of a digital computer, comprising software code portions for performing, when said product is run on

a computer, to carry out the invention of claim[[s]] 1 to 18.

21. (Original) A computer program product loadable into the internal memory of a digital computer, comprising software code portions for performing, when said product is run on a computer, to carry out the invention of claim 19.

22. (Currently Amended) A data processing apparatus for generating conditional electronic signatures, comprising:

one or more cryptographic components, responsive to one or more conditions (20) being specified for an electronic signature of a data item (10), for encrypting the data item (50), encrypting (50) the one or more conditions separately from the data item, combining (60) the encrypted data item and the encrypted one or more conditions, and encrypting the combination to generate a digital signature block (110) that inherently represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions; and

means for transmitting to a recipient the data item, the one or more conditions and the digital signature block (110).

23. (Currently Amended) A data processing apparatus for verifying a conditional electronic signature, generated by a method according to claim 10, comprising:

means for receiving the transmitted data item, one or more conditions and the digital signature block (110); and

one or more cryptographic components for: decrypting the digital signature block to produce a first result; encrypting the data item, encrypting the one or more conditions separately from the data item, and combining the encrypted data item and encrypted one or more conditions to produce a second result; and comparing the first and second results to determine whether they match.

24. (Original) A method for disseminating status information for conditionally signed data items, wherein the conditionally signed data items include executable content for updating a registry in response to one of the conditionally signed data items being forwarded to a recipient or being identified as rejected, the registry maintaining a list of recipients of the data item, the method including the steps of:

in response to forwarding of the conditionally signed data item to a new recipient, executing the executable content to update the list of recipients in the registry; and

in response to an indication that the conditionally signed data item is rejected, executing the executable content to update the registry and disseminating an indication that the data item is rejected to each of the recipients in the registry list.

25. (Original) A data processing apparatus for disseminating status information for conditionally signed data items, comprising:

a registry for maintaining a list of recipients of a conditionally signed data item;

means for recognizing the presence of an executable component within a conditionally signed data item and, responsive to the data item being forwarded to a new recipient, for

initiating execution of the executable component to update the list of recipients within the registry; and

means, responsive to an indication that the data item is rejected, for updating the registry to indicate the rejection and for disseminating an indication that the data item is rejected to each of the recipients in the list.

26. (Original) A computer program comprising program code instructions for controlling the operation of a data processing apparatus on which the program code executes, to perform a method according to claim 24.

**TRANSMITTAL LETTER TO THE UNITED STATES  
DESIGNATED/ELECTED OFFICE (DO/EO/US)  
CONCERNING A SUBMISSION UNDER 35 U.S.C. 371**

ATTORNEY'S DOCKET NUMBER

**GB920020055US1**

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)

INTERNATIONAL APPLICATION NO.  
**PCT/GB03/05107**

INTERNATIONAL FILING DATE  
**24 November 2003**

PRIORITY DATE CLAIMED  
**21 December 2002**

**TITLE OF INVENTION**

**METHODS, APPARATUS AND COMPUTER PROGRAMS FOR GENERATING AND/OR USING CONDITIONAL  
ELECTRONIC SIGNATURES AND/OR FOR REPORTING STATUS CHANGES**

**APPLICANT(S) FOR DO/EO/US**

**John Owlett et al.**

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a submission under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a submission under 35 U.S.C. 371.
3. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (24) indicated below.
4. ☒ The US has been elected (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c)(2))
  - a. ☐ is attached hereto (required only if not communicated by the International Bureau).
  - b. ☒ has been communicated by the International Bureau.
  - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
  - a. ☐ is attached hereto.
  - b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
  - a. ☐ are attached hereto (required only if not communicated by the International Bureau).
  - b. ☒ have been communicated by the International Bureau.
  - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
  - d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).
11. ☐ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A copy of the International Search Report (PCT/ISA/210).

**Items 13 to 23 below concern document(s) or information included:**

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A power of attorney and/or change of address letter.
19. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13<sup>ter</sup>.2 and 37 CFR 1.821 - 1.825.
20. ☒ A second copy of the published International Application under 35 U.S.C. 154(d)(4).
21. ☐ A second copy of the English language translation of the International Application under 35 U.S.C. 154(d)(4).
22. ☒ Express Mail Label No. **EV 594741016 US**
23. ☐ Other items or information:



Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

U.S. APPLICATION NO (if known, see 37 CFR 1.5)		INTERNATIONAL APPLICATION NO. PCT/GB03/05107		ATTORNEY'S DOCKET NUMBER GB920020055US1	
The following fees are submitted:				CALCULATIONS	PTO USE
24. <input checked="" type="checkbox"/> Basic national fee .....		\$300		\$	\$300.00
25. <input checked="" type="checkbox"/> Examination fee If International preliminary examination report prepared by USPTO and all claims satisfy provisions of PCT Article 33(1)-(4). ....		\$100		\$	\$200.00
All other situations. ....		\$200			
26. <input checked="" type="checkbox"/> Search fee .....					
Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority .....		\$100			
International Search Report prepared and provided to the Office .....		\$400			
All other situations. ....		\$500		\$	\$500.00
TOTAL OF 24, 25 and 26 =				\$	\$1,000.00
<input type="checkbox"/> Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing or computer program listing filed in an electronic medium). The fee is \$250 for each additional 50 sheets of paper or fraction thereof.					
Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof (round up to a whole)	RATE		
27 - 100 =	0 /50 =	0	x \$250.00	\$	\$0.00
Surcharge of \$130.00 for furnishing the oath or declaration later than months from the earliest claimed priority date (37 CFR 1.492(e)).				\$	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	26 - 20 =	6	x \$50.00	\$	\$300.00
Independent claims	4 - 3 =	1	x \$200.00	\$	\$200.00
MULTIPLE DEPENDENT CLAIMS (if applicable) <input type="checkbox"/> + \$360.00				\$	\$0.00
TOTAL OF ABOVE CALCULATIONS =				\$	\$1,500.00
<input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.				\$	\$0.00
SUBTOTAL =				\$	\$1,500.00
Processing fee of \$130.00 for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				\$	\$0.00
TOTAL NATIONAL FEE =				\$	\$1,500.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40 per property +				\$	\$40.00
TOTAL FEES ENCLOSED =				\$	\$1,540.00
				Amount to be	\$
				Amount to be	\$
a. <input type="checkbox"/> A check in the amount of \$ _____ to cover the above fees is enclosed.					
b. <input checked="" type="checkbox"/> Please charge my Deposit Account No. <u>09-0457 (IBM)</u> in the amount of <u>\$1,540.00</u> to cover the above fees. A duplicate copy of this sheet is enclosed.					
c. <input type="checkbox"/> The Director is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. _____. A duplicate copy of this sheet is enclosed.					
d. <input type="checkbox"/> Fees are to be charged to a credit card. <b>WARNING:</b> Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.					
NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.					
SEND ALL CORRESPONDENCE TO:					
Jack P. Friedman Schmeiser, Olsen & Watts 3 Lear Jet Lane, Suite 201 Latham, N.Y. 12110			SIGNATURE <u>Jack P. Friedman</u> NAME <u>44,688</u> REGISTRATION NUMBER		